Unique Factorization and Class Groups
TCU Seminar Lecture Notes

George T. Gilbert
Department of Mathematics, Texas Christian University
g.gilbert@tcu.edu

November 10, 17, & 29, 2011

1 Unique Factorization

Our rings R will be integral domains (with identity).

Definition. *$\alpha_1, \alpha_2 \in R$ are* **associates** *if $\alpha_1 = \alpha_2 u$ for some unit $u \in R$.*

Definition. *$\pi \in R$ is* **irreducible** *if $\pi = \pi_1 \pi_2$ implies either π_1 or π_2 is a unit.*

Definition. *R is a* **unique factorization domain** *(UFD) if every non-zero non-unit is a product of irreducible elements in a way that is unique up to order and associates.*

Examples: $\mathbb{Z}$, any field k, the polynomial ring $k[x_1, \ldots, x_k]$
GCDs exist in any UFD. (Greatest is in the sense of divisibility.)

Theorem. *If R is a UFD, then so is $R[x]$.*

Proof. Let R be a UFD and K its field of fractions. The **content** of $a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ is the GCD of $a_0, a_1, \ldots, a_n$. **Primitive** means content 1.

Lemma. *The content is multiplicative.*

Corollary. *(Gauss' Lemma) The product of primitive polynomials is primitive.*

Lemma. *A primitive polynomial is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.*

Now use that $K[x]$ is a UFD. □

Definition. *R is a* **principal ideal domain** *(PID) if every ideal has the form (α) for some $\alpha \in R$.*

Theorem. *In a PID R, a greatest common divisor g of α and β may be written as an R-linear combination of α and β.*

Proof. Let $(\alpha, \beta) = (\alpha) + (\beta) = (d)$. Thus, d is a divisor of α and β, hence $d|g$. Since (g) contains both (α) and (β), $d \in (\alpha) + (\beta) \subset (g)$. It follows $g|d$. Therefore d and g are associates and $(\alpha) + (\beta) = (g)$. □

This may be false in a UFD, e.g. look at x^2 and xy in $k[x, y]$.

Theorem. *Every PID is a UFD.*

Proof. Existence. We prove this more generally when in an integral domain when ideals are finitely generated (i.e. a **Noetherian domain**). If not, some non-unit α is infinitely divisible. This means there exists a sequence of elements $\alpha_1, \alpha_2, \ldots$ such that $(\alpha) \subsetneqq (\alpha_1) \subsetneqq (\alpha_2) \subsetneqq \ldots$. However, $\bigcup\limits_i (\alpha_i)$ is a proper ideal, hence finitely generated. The finite number of generators must all be contained in some (α_i), a contradiction.

Uniqueness.

Lemma. *(Euler's Lemma) If π is irreducible in a PID and π divides $\alpha\beta$, the π divides either α or β.*

Proof of lemma. (The lemma is nearly trivial for a UFD.) Let the irreducible π divide $\alpha\beta$. The ideal (π, α) is principal. A generator must divide π so must either be an associate of π hence π divides α, or a unit, hence $c\pi + d\alpha = 1$. Multiplying by β, we see π divides β.

The lemma extends immediately to all finite products. If our PID R is not a UFD, we have two factorizations of a non-unit in R with no factors of one associates of factors of the other. This contradicts the lemma. □

Note that $k[x, y]$ and $\mathbb{Z}[x]$ are UFDs but not PIDs.

Theorem. *Let R be a UFD. If, for every α and β in R, the GCD of α and β is an R-linear combination of α and β (R is* **Bezout domain***if $(\alpha) + (\beta)$ is always principal), then R is a PID.*

Proof. Suppose not. Take a non-principal ideal I. By the UFD property, there are principal ideals in I which are maximal with respect to inclusion. By assumption, all principal ideals in I are properly contained in I. Thus, there exists a non-principal subideal of I generated by two elements, α and β. However, the GCD of α and β generates $(\alpha) + (\beta)$. □

Definition. *R is a* **Euclidean domain** *if there exists a function $\nu : R - \{0\} \to \mathbb{Z}_{\geq 0}$ such that*
(i) For all $a, b \neq 0$, there exist q and r in R such that $a = qb + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.
(ii) $\nu(a) \leq \nu(ab)$.

Theorem. *Every Euclidean domain is a PID.*

Proof. Let I be a nonzero ideal. Take $\beta \in I$ such that $\nu(\beta)$ is minimal. For any $\alpha \in I$, let $\alpha = q\beta + r$ where $r = 0$ or $\nu(r) < \nu(\beta)$. Because $r \in I$, the latter is impossible. Therefore, $I = (\beta)$. □

Examples: $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\dfrac{1+\sqrt{5}}{2}\right]$

The latter two are **norm Euclidean**: one take ν to be the absolute value of the field norm (for quadratics $N(a+b\sqrt{d}) = a^2 - db^2$).

$\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID but is not Euclidean ([11], Theorem 4.18).

Fermat's Last Theorem asserts that $x^n + y^n = z^n$ has no solutions in positive integers for $n > 2$. Fermat used the formula for Pythagorean triples and descent to prove the case $n = 4$. Thus one need only establish the result for $n = p$ an odd prime. Results of Euler combine to prove the case $p = 3$ and the cases $p = 5$ and $p = 7$ followed fairly soon thereafter. These proofs depend on unique factorization in $\mathbb{Q}(e^{2\pi i/p})$.

Definition. *A* **Dedekind domain** *is an integral domain whose ideals are finitely generated (a* **Noetherian ring***), that is integrally closed, and for which non-zero prime ideals are maximal.*

In fact, every ideal is generated by at most two elements [9], p. 61 or [10], p. 136.

Theorem. *In a Dedekind domain, UFD implies PID.*

Proof. If a Dedekind domain R is a UFD but not a PID, consider an ideal $I = (\alpha, \beta)$ that is maximal with respect to inclusion among ideals requiring two generators. We may assume $I \subsetneqq (\gamma, \beta)$ if $(\alpha) \subsetneqq (\gamma)$. A GCD of α and β is 1 or else I would not be maximal. Let π be an irreducible factor of α. Because $(\alpha/\pi, \beta)$ must be a PID, it must be all of R. Thus, there exist c and d in R such that $c\alpha/\pi + d\beta = 1$. Hence $c\alpha + d\pi\beta = \pi$, so $\pi \in I$. But then (π) is a non-maximal prime ideal, a contradiction. □

Definition. *A* **number field** *K is a finite extension of $\mathbb{Q}$. Its* **ring of integers** *is the integral closure in K of $\mathbb{Z}$.*

When we talk about a number field having unique factorization, we mean its ring of integers has unique factorization.

Theorem. *The ring of integers in a number field is a Dedekind domain.*

Proof. One can use Galois theory to show that the ring of integers is integrally closed in its field of fractions.

The key to the rest is to show that the quotient by any nonzero ideal is finite. An ideal is prime if and only if its quotient ring is an integral domain. Finite integral domains are fields. An ideal is maximal if and only if its quotient ring is a field.

The ring of integers is a $\mathbb{Z}$-module of rank the degree of the extension over $\mathbb{Q}$. Every non-zero ideal has this same rank, so has finite index in the ring of integers, which equals the cardinality of the quotient ring. □

$\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD, so not all number fields have unique factorization.

In 1847, Lame published a "proof" of Fermat's Last Theorem [6]. Unfortunately, it assumed unique factorization in $\mathbb{Q}(e^{2\pi i/p})$, which is first false for $p = 23$. This led Kummer to develop a theory of ideals.

Theorem. *In a Dedekind domain, nonzero proper ideals can be written uniquely (up to order) as the product of prime ideals.*

For a proof, see [9], [10], or [7]. The converse is also true.

2 Class Groups of Number Fields

Lame's failed proof of Fermat's Last Theorem in 1847 [6] led to Kummer's development of the theory of ideals in an attempt to get around the lack of unique factorization.

Changing focus momentarily, binary quadratic forms $ax^2 + bxy + cy^2$ over the integers are equivalent if one can be transformed into the other by a unimodular linear transformation. This partitions the forms with a fixed discriminant. Gauss proved the number of equivalence classes is finite.

It turns out that for a positive definite form, the number of classes is the class number of the corresponding imaginary quadratic field, defined below.

Definition. *A* **fractional ideal** *M in a Dedekind domain R is an R-module of the form $\alpha^{-1}I$ where I is a nonzero ideal of R and α is a nonzero element of R. Equivalently, it is an R-module M in the field of fractions for which there exists a nonzero element α of R for which αM is an ideal.*

Theorem. *In a Dedekind domain, the fractional ideals form a group.*

Proof. The only issue is inverses. Let K be the field of fractions. One can show $M^{-1} = \{\beta \in K : \beta M \subset R\}$. The converse is also true. □

Definition. *The* **class group** *is the quotient group of fractional ideals by principal ideals.*

You can avoid fractional ideals by defining ideals I and J to be equivalent if there exist nonzero α and β in R such that $\alpha I = \beta J$. Using techniques from the geometry of numbers, one can prove ([1], [7], or [9])

Theorem. *The class group of a number field is finite.*

Theorem. *(Kummer) If the class number of $\mathbb{Q}(e^{2\pi i/p})$ is not divisible by p (p is a* **regular** *prime), then Fermat's Last Theorem holds for exponent p.*

Although it is conjectured that about 60% of all primes are regular, it is not even known whether there are infinitely many regular primes, only that there are infinitely many irregular primes.

We've seen that the class number for $\mathbb{Q}(\sqrt{5})$ is 1. For $\mathbb{Q}(\sqrt{-5})$, it is 2. Exercise for graduate students: Prove $(3, 1+\sqrt{-5})^2$ is principal in $\mathbb{Z}[\sqrt{-5}]$. (Warmup: Prove $(2, 1+\sqrt{-5})^2$ is principal in $\mathbb{Z}[\sqrt{-5}]$.) For $\mathbb{Q}(e^{2\pi i/23})$, it is 3. For $\mathbb{Q}(e^{2\pi i/97})$, it is $411,322,824,001 = 577 \cdot 3457 \cdot 206209$. [1]

There are analytic formulas for the class number. In general, the class number h of the number field K is given by ([1], p. 319)

$$h = \frac{w\sqrt{|D|}}{2^{r+t}\pi^t \mathrm{Reg}} \lim_{s \to 1^+} (s-1)\zeta_K(s),$$

where w is the order of the finite (torsion) part of the group of units, D is the discriminant (a measure of the size of the lattice of the ring of inetgers), r is the number of real embeddings of K and $2t$ is the number of complex embeddings of K, Reg is the regulator (a measure of the size of the multiplicative lattice of units), and $\zeta_K(s)$ is the Dedekind zeta function of K. Another way to view this is that the residue of the zeta function at 1 encodes arithmetic information. Interestingly, nonisomorphic fields may have the same Dedekind zeta function and the zeta function does not even determine the class number [2].

In the case of an imaginary quadratic field, further calculation leads to to the Dirichlet class number formula [5] for the class number h of $Q(\sqrt{-d})$, where d is the fundamental discriminant and $\left(\frac{-d}{m}\right)$ is the Kronecker (generalized Legendre) symbol:

$$h = \frac{w}{2d} \sum_{m=1}^{d} m \left(\frac{-d}{m}\right).$$

For $Q(\sqrt{-d})$, the class number goes to ∞ as d does. However the first proofs were ineffective. It was known for a while that nine imaginary quadratic fields have class number one and that there is at most one more. In 1966, Baker and Stark independently and by different methods proved that there are no others. They went on to determine the fields with class number two in 1971. "Effective" bounds are due to Goldfeld, Gross, and Zagier. Today, all imaginary quadratic fields up to class number 100 are now known [12]. On the other hand, it is not known whether there are finitely many or infinitely many real quadratic extensions with class number one. Cohen-Lenstra predict that about three-fourths of real quadratic fields will have class number one. The generalized Riemann hypotheses has a bearing on these questions.

Theorem. *(Carlitz, 1960 [3]) An algebraic number field K has class number at most two if and only if the length of a decomposition of an algebraic integer $\alpha \in K$ into irreducible factors depends only on α.*

Proof. We begin with a more general observation. Suppose we have a Dedekind domain, where nontrivial ideals factor uniquely (up to order) as the product of prime ideals. Express (α) as the product of prime ideals. Then α is irreducible if and only if no nonempty product of a subset of these prime ideals is principal.

Let R be the ring of integers in a number field and first suppose R has class number two. Factor a nonzero, non-unit α into a product of irreducibles $\alpha = \pi_1\pi_2 \cdots \pi_k$. Some of these irreducibles, say $\pi_1, \ldots, \pi_j$, generate prime ideals. An associate of each of these must appear in any factorization of α into irreducibles, i.e. j depends only on α, not on the particular factorization. By our observation, the rest factor into a product of two prime ideals. Thus the length of the factorization of (α) into a product of prime ideals is $j + 2(k - j) = 2k - j$, hence k depends only on α.

For the converse, we need the nontrivial fact that each class of ideals contains a prime ideal. If the class group has an element of order m greater than 2, we may take a prime ideal $\mathfrak{p}$ in this class and a prime ideal $\mathfrak{p}'$ in its inverse class. Then $\mathfrak{p}^m = (\pi_1)$ and $(\mathfrak{p}')^m = (\pi_2)$, where π_1 and π_2 are irreducible. Also $\mathfrak{p}\mathfrak{p}' = (\pi)$, where π is irreducible. However, we now have $\pi_1\pi_2 = \varepsilon\pi^m$, where ε is a unit.

For the last case of the converse, we have nonprincipal prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ with $\mathfrak{p}_j^2 = (\pi_j)$, with π_j irreducible, and $\mathfrak{p}_3 \sim \mathfrak{p}_1\mathfrak{p}_2$ in the class group. The latter implies $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (\pi)$, where π is irreducible. Thus $\pi_1\pi_2\pi_3 = \varepsilon\pi^2$, where ε is a unit.

□

In a similar spirit, there is a characterization of number fields with class number 3 or less due to Chapman and Smith [4].

References

[1] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, 1966.

[2] W. Bosma and B. de Smit, " "On arithmetically equivalent number fields of small degree," in Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Computer Science 2369, Springer 2002, 67–79, MR2041074.

[3] L. Carlitz, "A characterization of algebraic number fields with class number two," Proc. Amer. Math. Soc. 11 (1960), 391–392, MR0111741.

[4] S. T. Chapman and W. E. Smith, "On a characterization of algebraic number fields with class number less than three," Journal of Algebra 135:2 (1990), 381–387, MR1080853.

[5] H. Davenport, Multiplicative Number Theory, 3rd ed., Springer, 2000.

[6] G. Lame, "Demonstration general du theoreme de Fermat," Comptes Rendus 24 (1847), 310-315.

[7] S. Lang, Algebraic Number Theory, Addison-Wesley, 1977. (There is a newer 1994 Springer edition.)

[8] H. W. Lenstra, Jr., "On Artin's conjecture and Euclid's algorithm in global fields", Inventiones Math. 42 (1977), 201-224, MR0480413.

[9] D. Marcus, Number Fields, Springer-Verlag, 1977.

[10] R. Mollin, Algebraic Number Theory, Chapman & Hall, 1999.

[11] I. Stewart and D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd edition, A. K. Peters, 2002.

[12] http://bourwiki.org/wiki/Archive:A000159#S_3_2